Develop Your Information Security Management System
Processes: The S&R Practice Playbook
by Laura Koetzle and Renee Murphy
January 19, 2017

Why Read This Report
The chief information security officer’s (CISO) role is fraught with many challenges, including more sophisticated adversaries, a larger attack surface, increasing regulation, and customer demands. Stretched in so many directions, the CISO can easily neglect the fundamental processes by which the security team identifies, evaluates, and treats security risks. This report describes how to use an information security management system (ISMS) to drive risk ownership, continual improvement, and deep business engagement.

This is an update of a previously published report; Forrester reviews and updates it periodically for continued relevance and accuracy.

Key Takeaways

**CISOs Often Focus On Controls Instead Of Risk Management**
Cherry picking controls from various frameworks to handle specific problems can deliver quick wins but does not result in a comprehensive security program that the firm can rely on.

**An ISMS Establishes A “Virtuous Circle” To Resolve Security Issues**
An ISMS is not a list of controls, a set of policies, or a program maturity model — it is a systematic approach to managing your information so that it remains secure. Your ISMS will guide an iterative process for identifying risks from a variety of sources, drawing them in for analysis and treatment.

**Regular Business Engagement Encourages Prioritization And Budgetary Support**
When business leaders are part of the guiding forum, the security strategy naturally reflects business imperatives and the organization’s risk tolerance; this ensures that the security team can focus their efforts on the initiatives that win, serve, and retain customers.
Develop Your Information Security Management System
Processes: The S&R Practice Playbook

by Laura Koetzle and Renee Murphy
with Stephanie Balouaras, Christopher McClean, Claire O’Malley, Trevor Lyness, and Sam Bartlett
January 19, 2017

Table Of Contents

2 Digital Transformation And Business Visibility Demand More Of CISOs
   CISOs Often Focus On Controls Instead Of Risk Management

3 Build An ISMS To Strengthen Security Processes And Business Support
   Address All Components Of An ISMS
   Establish A “Virtuous Circle” To Resolve Security Issues

7 Commitment To A Full ISMS Implementation Yields Clear Value
   Make The ISMS Day-To-Day Business To Keep The Benefits Coming

What It Means

8 The Process Is As Important As The Results

Notes & Resources

Forrester interviewed multiple vendor and user companies. In addition, we drew from a wealth of analyst experience, insight, and research through review of existing frameworks.

Related Research Documents

Defend Your Digital Business From Cyberattacks Using Forrester’s Zero Trust Model
Extend Compliance And Risk Management To What Really Matters For Your Business
Forrester’s 2016 Interactive Data Privacy Heat Map
Digital Transformation And Business Visibility Demand More Of CISOs

Although security incidents are nothing new, the business world now sees the potentially devastating impacts of such events in terms of brand damage, lost customers, and lost revenue — and the regulators and legislators are active.¹ In response, top executives and board members expect their security leaders to have a plan, an arsenal of tried and tested processes to protect their firm and its customers. And that’s a tall order for CISOs. Here’s why:

› **Attackers refine their craft — and they only have to succeed once.** One of the unalterable facts of modern information security is that it’s asymmetric — attackers can try and fail a thousand times until they find a single vulnerability to exploit, while defenders must succeed every day. And because intellectual property and customer data are easy to monetize on the black market, organized cybercriminal syndicates have no trouble attracting talented hackers.²

› **Digital business has no perimeter.** Your digital business follows your customers, employees, and partners wherever they need access to your data and services. This makes your attack surface both large and volatile — and requires a Zero Trust approach for which many CISOs find their companies’ infrastructure unprepared.³

› **Fast-and-furious customer data breaches make CISOs’ efforts look futile.** Security budgets climbed from 22% of technology budgets in 2014 to 28% in 2016.⁴ But despite the increased spending, companies racked up 2.2 billion breached records in the first 10 months of 2016.⁵ If CISOs can’t explain how their countermeasures will help protect the firm — while setting the expectation that breaches may still occur — they’ll quickly lose support.

CISOs Often Focus On Controls Instead Of Risk Management

The majority of security functions have adopted some kind of framework to organize and guide their actions. This demonstrates a focus on formal processes and documentation; however, security leaders are still battling the same issues. Why? It’s because:

› **Organizations are cherry picking controls.** Many CISOs cherry pick elements of the various standards they deem suitable to their particular environment. Organizations that claim to use ITIL, for example, typically just adopt the core elements of incident and change management.⁶ This piecemeal approach may appease some auditors and regulators, but it doesn’t give a firm a comprehensive security program.

› **Certain frameworks perpetuate negative perceptions of security as a roadblock.** Standards such as the PCI DSS are prescriptive, requiring a set of predefined controls — which makes them easier to build compliance checklists for than principles-based frameworks like the new EU General Data Protection Regulation (GDPR) that will come into force in May 2018.⁷ When used poorly, prescriptive standards perpetuate the idea of information security as a discipline that “follows the letter of the law” at minimal cost and effort, rather than as a methodology for understanding and managing risk.
› **Every framework has a point of view and a particular scope.** For example, COBIT focuses on IT governance, while ITIL's roots are in service management. These frameworks can be valuable tools; however, their precise applications may not be suitable for addressing a wide range of information risks.

### Build An ISMS To Strengthen Security Processes And Business Support

CISOs must establish and test formal processes to manage priorities, direct resources more economically, and transform reactive and ineffective efforts. An ISMS is the best way to organize all of these security efforts and investments into a cohesive program.

### Address All Components Of An ISMS

An ISMS is not a list of controls, a set of policies, or a program maturity model — it is a systematic approach to managing your information so that it remains secure. If you want a model to help you define the roles, responsibilities, and functions of your entire security program and assess its maturity, Forrester recommends our own Information Security Maturity Model. However, to guide a successful ISMS implementation, ISO 27001 is your best bet; it is the most frequently used and most complete model (see Figure 1):
## FIGURE 1 Key Components Of An ISO 27001 Information Security Management System

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security policy and awareness</td>
<td>A set of policy documents outlining the organization’s stance on information security issues and defining acceptable user behavior. These policies are accompanied by a delivery mechanism to ensure that staff are kept aware of their responsibilities.</td>
</tr>
<tr>
<td>Incident register</td>
<td>A document and process to record each security-related incident. This should quantify the impact of the incident while highlighting root causes and learning opportunities. It’s important that this is not just for IT incidents; it must include all information-security-related issues (e.g., misdirected email, client documentation left on a train, etc.).</td>
</tr>
<tr>
<td>Risk assessment process</td>
<td>A process to review and assess the likelihood of any particular risk issue, together with the vulnerability and subsequent impact to any particular asset. This should be an agile, rapid, and repeatable process.</td>
</tr>
<tr>
<td>Baseline risk assessment</td>
<td>A recurrent and comprehensive document that details the risks across the organization. This will have been created using the risk assessment process above.</td>
</tr>
<tr>
<td>IT audit process</td>
<td>A process, schedule, and mandate to review processes, teams, and technology configurations across IT and, perhaps, the wider business and extended enterprise. This process must include a methodology for identifying the “desired state” to be audited against, often derived from compliance requirements or best-practice standards. Vulnerability scanning tools and penetration testing are included here, as are external audits.</td>
</tr>
<tr>
<td>Key performance indicators</td>
<td>To indicate the effectiveness of any control, or the adherence to any process or policy, a measurement is required. This is a collection of metrics that can provide insight into the level of control and compliance across the organization.</td>
</tr>
</tbody>
</table>
FIGURE 1 Key Components Of An ISO 27001 Information Security Management System (Cont.)

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information security forum</td>
<td>A regular, scheduled meeting of key individuals representing both IT security and the business, usually chaired by the CISO. This group is core to the success of an ISMS and will make key decisions on risk issues, including risk acceptance and policy approval. This body can request the completion of specific risk assessments and audits; it can also make proposals for investment to the management board. The CISO is commonly empowered to act on behalf of the forum in day-to-day and time-critical issues.</td>
</tr>
<tr>
<td>Risk register/treatment plan</td>
<td>The central document that drives the ISMS. This is a simple spreadsheet that lists all current risks together with their risk level, action plan, and owner. The document records treated, accepted, and project risks together with any third-party-related risks. It also commonly records policy exceptions. This is the schedule that drives risk mitigation actions and enables CISOs to step back, look at the wider picture, and act strategically.</td>
</tr>
<tr>
<td>Threat awareness and intelligence</td>
<td>A collection of processes, tools, and sources to understand the current threat environment and how it applies to the organization’s assets. This can include information from IDS systems, vulnerability analysis tools, and security operations centers (SOCs), as well as peer discussion forums, government insight, and professional threat intelligence services.</td>
</tr>
<tr>
<td>Information risk strategy and strategic program</td>
<td>The overarching strategic mission statement that directs the information risk practice, and the supporting program, projects, and initiatives that drive its implementation.</td>
</tr>
</tbody>
</table>

Establish A “Virtuous Circle” To Resolve Security Issues

Your ISMS will guide an iterative process for identifying risks from a variety of sources, drawing them in for analysis and treatment, and managing them to a level where the organization can accept them and drop them out of the sequence (see Figure 2). There are several ways this might work for your organization:

› Example No. 1: Update a policy to reduce a low-level risk. Say a baseline risk assessment determines that your firm lacks any form of USB encryption software, which could risk exposure of sensitive or customer data. You enter this information into the risk treatment plan and report it to the security forum, which requires an IT audit of use of USB sticks. The audit shows a low level of USB usage — because employees primarily use Box to transfer such data. Thus, the security forum declines to invest in a technical control. Instead, it issues a new policy prohibiting the use of USBs for sensitive or customer data and amends the risk treatment plan to show the risk as “accepted, to be reviewed in 12 months.”
› **Example No. 2: Invest in technology to close an audit finding.** Consider a scenario in which an audit determines that the operations department cannot meet customer demand for website availability. The internal auditors enter their recommendation into the risk treatment plan, with the remedial action owned by operations. Operations states that their current data center setup cannot support continuous operation, so they cannot comply. The security forum receives the report from operations and considers the risk of nonavailability, deciding to fund a migration to a public cloud platform. The operations department performs the migration, and a brief IT audit confirms the change. Within the risk treatment plan, the CISO denotes the risk as “treated” and advises the security forum at the next opportunity.

› **Example No. 3: Make an informed decision to accept the risk of a new threat.** Here, your security analytics solution uncovers an increase in attack activity. Acting on behalf of the security forum, the CISO immediately calls for a risk assessment and finds that the target is a seldom-used website. The security team conducts a penetration test and finds no exploitable vulnerabilities. The CISO advises the security forum, which formally agrees to amend the risk treatment plan to accept the risk while asking the CISO to monitor the threat intelligence service and security analytics platform output for the coming month.
Commitment To A Full ISMS Implementation Yields Clear Value

The ISMS model focuses on risks rather than controls and on business needs rather than technical details. As many organizations have shown, implementation of an ISMS has the potential to lead the CISO to a new, proactive way of working. The benefits are clear:

- **Regular business engagement encourages prioritization and budgetary support.** When business leaders are part of the guiding forum, the security strategy naturally reflects business imperatives and the organization’s risk tolerance; this ensures that the CISO has management support and helps the security team align with efforts to win, serve, and retain customers and drive business growth.11
› **A workflow based on continual improvement drives down risk.** The constant review cycle of the ISMS ensures that the security team adopts a culture of continual improvement. This insulates the firm against repeated audit findings because the ISMS process identifies the most critical issues and addresses them with business buy-in and prioritization.

› **After the initial investment of effort, the team becomes more effective.** An ISMS requires no specific technology investment, but it does demand that security leaders allocate sufficient time, training, and change management effort to ensure that it is effective.

### Make The ISMS Day-To-Day Business To Keep The Benefits Coming

CISOs should engage their teams in every stage of the development of the ISMS processes and drill them in until they become automatic. The ISMS isn't just a management framework; it's a philosophical choice that changes how your team behaves. Adopt a reference notation system in each of the input processes, and tie this to the numbering scheme in your risk treatment process. Diligence here will build an audit trail that will satisfy auditors, enabling them to track issues from detection, through decision and treatment, and to the ultimate resolution.

### What It Means

**The Process Is As Important As The Results**

Internal and external stakeholders will always want CISOs to reduce risk effectively; they'll also want to feel confident that you can achieve those reductions by consistently following a sound process. After all, it's hard for stakeholders to trust a report touting the number of risks you've mitigated if they don't trust the processes by which you discover risks in the first place. Executives and boards of directors, especially, are concerned that their firm's security efforts don't let problems fall through the cracks. Regulators and auditors, too, will have a better impression of companies that have formal, documented, and tested risk management processes in place.
Engage With An Analyst

Gain greater confidence in your decisions by working with Forrester thought leaders to apply our research to your specific business and technology initiatives.

Analyst Inquiry
To help you put research into practice, connect with an analyst to discuss your questions in a 30-minute phone session — or opt for a response via email.

Learn more.

Analyst Advisory
Translate research into action by working with an analyst on a specific engagement in the form of custom strategy sessions, workshops, or speeches.

Learn more.

Webinar
Join our online sessions on the latest research affecting your business. Each call includes analyst Q&A and slides and is available on-demand.

Learn more.

Forrester’s research apps for iPhone® and iPad®
Stay ahead of your competition no matter where you are.

Endnotes

1 Although many business demands and legal requirements necessitate the collection and use of personal information and data, organizations must carefully control how they handle such data to preserve individuals’ privacy rights. Many countries have enacted data privacy regulations stipulating the conditions under which organizations can collect, process, and store personal data; these regulations also guide relevant issues such as the requirements and limitations on data transfer across countries. See the Forrester report “Forrester’s 2016 Interactive Data Privacy Heat Map.”

2 In today’s threat landscape, skilled, well-funded, organized cybercriminals are working to steal your data — the lifeblood of your digital business — in pursuit of economic, political, or military gain. To combat this, security and risk (S&R) leaders need Forrester’s Zero Trust Model of information security. With Zero Trust, S&R leaders develop robust detection and incident response capabilities and deploy security throughout the digital business ecosystem. To learn more about how to defend your customers with the Zero Trust Model, please see the Forrester report “Defend Your Digital Business From Cyberattacks Using Forrester’s Zero Trust Model.”

3 One of Forrester’s goals with Zero Trust is to optimize the security architectures and technologies for future flexibility. As we move toward a data-centric world with shifting threats and perimeters, we look at new network designs that integrate connectivity, transport, and security around potentially toxic data. For more information, see the Forrester report “Build Security Into Your Network’s DNA: The Zero Trust Network Architecture.”
S&R professionals continue working their way into positions of greater authority and influence in their organizations. However, they still struggle at times to understand the full scope of their responsibilities, prioritize their initiatives, develop a coherent strategy, and articulate their value to the business. In response to these challenges, we have developed the Forrester Information Security Maturity Model. This comprehensive framework will allow you to identify the gaps in your security program and portfolio, evaluate the program’s maturity, and better manage your security strategy. The model consists of four top-level domains, 25 functions, and 128 components, each with detailed assessment criteria; it provides a consistent and objective method to evaluate security programs and articulate their value. For more information, see the Forrester report “Assess Your Security Program With Forrester’s Information Security Maturity Model.”

Examples of security aligning with the business include protecting new digital business channels, implementing better customer-facing authentication techniques, or solidifying customer loyalty with a transparent privacy policy. See the Forrester report “CISOs Need To Add Customer Obsession To Their Job Description.”

The first step is to choose the best treatment options to pursue for each risk or combination of risks that you understand to be outside of your risk tolerance. The choice will depend on the information gathered during the evaluation stage of the risk management process, with several factors to consider. See the Forrester report “The Risk Manager’s Handbook: How To Plan And Execute Appropriate Risk Treatment.”
We work with business and technology leaders to develop customer-obsessed strategies that drive growth.

PRODUCTS AND SERVICES
› Core research and tools
› Data and analytics
› Peer collaboration
› Analyst engagement
› Consulting
› Events

Forrester’s research and insights are tailored to your role and critical business initiatives.

ROLES WE SERVE
Marketing & Strategy Professionals
- CMO
- B2B Marketing
- B2C Marketing
- Customer Experience
- Customer Insights
- eBusiness & Channel Strategy

Technology Management Professionals
- CIO
- Application Development & Delivery
- Enterprise Architecture
- Infrastructure & Operations
- Security & Risk
- Sourcing & Vendor Management

Technology Industry Professionals
- Analyst Relations

CLIENT SUPPORT
For information on hard-copy or electronic reprints, please contact Client Support at +1 866-367-7378, +1 617-613-5730, or clientsupport@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.